



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487.502	01/19/2000	Cynthia Dwork	AM9-99-0138	3238

7590

04/05/2005

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER

KLIMACH, PAULA W

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/487,502	Applicant(s) DWORK ET AL.	
	Examiner Paula W Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 July 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to Appeal Brief filed on 07/06/04. Original application contained Claims 1-35.

Response to Arguments

Applicant's arguments filed 07/06/05 have been fully considered. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Presented below are the new grounds of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 12, and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by the paper by Goldreich et al.

As per claim 1, Goldreich discloses a signature scheme (page 3 paragraph 6) comprising: generating a lattice L having at least one short basis establishing a private key and at least one long basis establishing a public key (section 3.3); mapping at least the message μ or a concatenation thereof to a message point “x” in n-dimensional space using a function “f”

rendering infeasible the possibility of mapping two messages together in the space (section 1.2 page 3 paragraphs 5-6 “Our signature scheme”); and using the short basis, finding a lattice point of the lattice L that is close to the message point (page 18 section 5 especially section 5.1).

As per claim 2, the limitation of returning the message point x and the lattice point y as the digital signature, returning both the message point and the lattice point is necessary in order to verify the signature and further determine the authenticity of the message.

As per claim 12, the additional limitation of computer code for mapping a message or a concatenation thereof to a message point in n -dimensional space, the message point being a point of a grid or a point of an auxiliary lattice (page 10 section 3.3); computer readable code means for finding a point of a key lattice that is not the same as the auxiliary lattice (page 11 section 3.3.2); and computer readable code means for establishing a digital signature, based at least on the earlier mentioned points (page 18 section 5).

As per claim 26, the limitation of generating a lattice having at least one short basis and at least one long basis disclosed in Goldreich page 8, section 3.1 “Generate.” A mapping that maps at least the message to a message point in n -dimensional space, the message point x being an element of a set spaced points not on the lattice (page 18 section 5.1 “Signature”). The limitation of using the short basis to find a lattice point in the lattice that is within a predetermined distance of the message point (page 18 section 5.1 “signature”).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3-11, 13-25, 27-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldreich in view of Diffie/Hellman.

In reference to claim 19, Goldreich discloses a system capable of producing digital signature for an electronic message; see discussion in claim 1. Creating a message and representing as a point on the public key basis as x and creating a lattice point y on the private key basis which are a predetermined distance apart are disclosed in Goldreich see discussion in claim 1.

Transmitting the message and x and y and determining the distance between x and y at a remote site fall within the predetermined distance are disclosed in Diffie/Hellman as the function of any public key telecommunication system (see introduction especially first and second paragraph column 1).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have combine these separate aspects into a single secure communication system because as Diffie/Hellman discuss in the first paragraph of the introduction, "we stand today on the brink of revolution in cryptography which will be able to exploit these aspects in a modern telecommunication environment. Claim 19 is rejected.

As per claim 3, further comprising randomizing the function f. Diffie/Hellman note

Art Unit: 2135

(page 36, column 2, second paragraph) that a one way function f is a building function to both encryption functions (e.g. block ciphers) and key generators (pseudorandom sequence).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have continually changed the function f in a random fashion, because all pseudorandom sequences have periods from which the function f can be determined. One of ordinary skill in the art would have been motivated to do this because randomly changing this function permits the use of this function over a lengthy period of time without compromising the cryptosystem

As per claims 4 and 28, the limitation that the message f is randomized by concatenating the message u with a random number p . Diffie/Hellman note (last paragraph, column 2) that cipher text only attacks succeed because the cryptanalysis knows the statistical properties of a language or certain probable words or more generally certain message formats (called cribs) that enable the cryptanalysis to establish certain correspondence between cipher text and plaintext. The use of nulls, as it was known in the nineteenth century or padding or salting (especially for passwords), adds random text to the message to prevent such attacks from working.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have padded messages with random text (numbers). One of ordinary skill in the art would have been motivated to do this because to prevent the earlier mentioned attacks.

As per claims 5 and 29, the limitation that the function f maps the message u to a point on a grid disclosed by Diffie/Hellman page 35, column 2 paragraph 2. Diffie/Hellman disclose for the functions suitable for f sparse polynomials over finite field. Thus f maps u to a point in the

Art Unit: 2135

range space of f . Both the domain and range spaces would constitute a finite grid and hence the limitation is met. Claim 5 is rejected.

As per claims 6, 8, 30, and 32 the limitation that the function f may be collision intractable is disclosed page 35 second to last paragraph in particular "we are defining a function which is not invertible from a computational point of view. Certainly an invertible function is collision intractable and if in addition its inverse is computationally difficult it would serve as a one way function. Further in the same paragraph Diffie/Hellman consider the case of a one way function which has $f(x_1) = y = f(x_2)$ that is they are computationally intensive and have collisions that is for a single y , $x_1 = x_2$.

Thus one of ordinary skill in the art at the time the invention was made would have considered forms of f that satisfy both of these conditions in order to increase the security in the case of the collision intractable case or increase flexibility in the case that f allows collisions. Claims 6 and 8 are rejected.

As per claims 7 and 31, the limitation that the collision intractability of f is based on a computational hard problem such as a lattice problem, Diffie/Hellman have pointed out that the one way function f are based on overwhelmingly difficult (hard) problems (see column 1 bottom page 35, Diffie/Hellman explain what they mean by overwhelmingly difficult in section 6 in terms of NP complexity) and Goldreich teach lattice problems as computationally hard for computing the digital signature.

Thus one of ordinary skill in the art at the time the invention was made would have been motivated to apply the teachings of Diffie/Hellman to the invention disclosed by Goldreich

Art Unit: 2135

because the encryption system already has the lattice problem in place either in software or hardware or both.

As per claims 9 and 33, the limitation that the function f maps the message u to an auxiliary lattice. Diffie/Hellman disclose that the hard over which the Encryption function (i.e. hard lattice problem disclosed by Goldreich) does not have to be the same in which the function f is based (that is sparse polynomials over a finite field Diffie/Hellman page 35 second comment see Purdy comment), and thus one of ordinary skill in the art at the time the invention was made would have not necessarily been motivated to base both the encryption function and the hashing function on the same hard problem (that is the same lattice or different lattice problems) for security reasons. One might leak more information (bits) in the hashing process than in the encryption process or vice versus and thus might have to use different lattices or even different lattice problems, entirely.

As per claims 10 and 34, the limitation of verifying the digital signature by determining whether the distance between the lattice point x and y vary no more than a predetermine amount. Goldreich teaches the closest vector problem wherein when given a basis for a lattice, the task is to find the vector that is closest to v (page 6 section 2.1).

As per claims 11 and 35 that the predetermined distance is related to the number of dimensions n in the lattice, see Goldreich page 10 section 3.3.1.

Claims 13-15 and 17-18 with the limitation addressed above, are directed towards a computer program storage device with instructions to implement the method claims 1, 6, 3, 4 and 8-9, and are therefore rejected in view of the same prior art of record.

As per claim 16, the limitation that f maps the message to a point on a grid was addressed in 5, the limitation of collision intractable was addressed in claim 6 and finally the intractability being based on the hardness of the lattice problem was address in claim 7. It would have been obvious for one of ordinary skill in the art at the time the invention was made to have been motivated to combine these features because they each add to the overall security and ease of implementation of the encryption device.

Claims 20-25 are system limitations incorporated the limitations of claims 16, 4, 6-8, and 11 and are rejected with the same rationale.

As per claim 27, the limitation that the mapping is undertaken using a function f is met as a mathematical truism. For example see the CRC Concise Encyclopedia of Mathematics by Eric W. Weissten page 1136. The terms FUNCTION and MAPPING are synonymous with map. Even if this were not considered Goldreich as modified by Diffie/Hellman disclose that the mapping process is via a one way function f which in from the standpoint of Diffie/Hellman is necessary in order to determine data integrity (page 35 second column), authenticity (page 35 second column) and data security (privacy page 30, bottom and continuing to the second column).

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, April 01, 2005


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100